DETAILED ACTION

1. The following is a first office action upon examination of application number 10/729,814. Claims 1-15 are pending in the application and have been examined on the merits discussed below.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on December 5, 2003 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 6 and 8-11 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 6 cites a computer system comprising means for performing a plurality of steps. However, claim 6 does not recite the requisite structure (i.e., computer hardware) typical of a system claim; thus, the "means for" are interpreted as software per se because they are not embodied on a computer-readable or computer-executable medium. Although claim 6 recites that the claimed computer system includes "computer

software recorded on a computer-readable medium", without the requisite system structure, the claim is interpreted as being solely software per se, which is not statutory.

A software program not embodied on computer-readable or computer-executable medium is software per se. Software, programming, instructions or code not claimed as embodied in computer-readable media are descriptive material per se and are not statutory because they are not capable of causing functional change in a computer. When such descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases. Claim 6 does not utilize the proper computer program format and effectively recite descriptive material (software) per se. Claims 6, and 8-11 are therefore deemed to be directed to non-statutory subject matter where there is no indication that the proposed software is recorded on computer-readable medium and/or capable of execution by a computer.

Furthermore, software, programming, instructions or code not claimed as being computer executable are not statutory because they are not capable of causing functional change in a computer. In contrast, when a claimed computer-readable medium encoded with a computer program defines structural and functional interrelationships between the computer and the program, and the computer is capable of executing the program, allowing the program's functionality to be realized, the program will be statutory. For example, if each of the claimed "means for" steps were

claimed to have being embodied within a processor (i.e., "processing means for constructing...." or "a processor, comprising means for constructing...., means for calculating.,,,, and means for selecting...."), then the claimed invention would provide a structural and functional interrelationship between "means for" and claimed computer system.

Claims 8-11 are dependent on claim 6 and thus are also rejected.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan et al. (US Patent #6,889,375) in view of Hung Chak Kuen Patrick's "Secure Workflow Model" (provided as reference 1-U, hereinafter referred to as Patrick).

As per claim 1, Chan et al. teaches a method for selecting a workflow, said method comprising the steps of:

(a) constructing a set of possible workflows meeting a workflow specification having a predetermined input and a required output, using components having defined inputs and outputs **(A display 148 presents icons representing workflows 108 and**

workflow steps 109 in an editor window 150, enabling a user to easily create and edit workflows 108. Contracts 102a specify interactions between design-time container 110 and workflows 108 and workflow steps 109 typically by describing service that design-time container is to provide to workflow steps 109. For example, a contract 102a specifies that design-time container 110 is to retrieve workflow steps 109 for workflow 108 by associating workflow 108 with the retrieval of workflow steps 109. Another contract 102a specifies that design-time container 110 is to retrieve input data from a user for workflow step 109 by associating workflow step 109 with the retrieval of input data.....Application server 128 includes a workflow repository 132, a workflow administrator 130, and run-time container 112. Workflow repository 132 stores workflows 108 and contracts 102c associated with the workflows. Contracts 102c specify interactions between workflows 108 and workflow steps 109. For example, a workflow step 109 is designed to retrieve a file and includes a file name variable. An instantiation of workflow 108, called a task, supplies the file name value to be used for the file name variable. A contract 102 specifies the file by associating the file name variable of workflow step 109 and the file name value of the task) [Column 3, lines 28-39, 45-55];

Although not explicitly taught by Chan et al., Patrick teaches the steps of:

(b) calculating a predetermined exposure measure for each of the possible workflows in the set of possible workflows **(Security Risk Factor - the maximum**

number of tasks done by any one agent. Essentially, the SRF measure the level of risk associated with a set of agents executing a group of inter-dependent tasks; Security Risk Factor…is based on evenly distributing the tasks over a set of agents with the condition that all the agents are capable of executing all the tasks and all of them can access the documents with the different privileges needed by each task…. We introduce the concept of Security Risk Value and incorporate it into SRF. SRV is a value from 0 to 1.0 that indicates the level of risk. The higher the value, the higher is the risk) [pages 73, 79, 96]; and

(c) selecting the constructed set of possible workflows for which the predetermined exposure measure is calculated to be a minimum **(When statically assigning tasks (and the associated privileges) to agents, the principle of least privilege dictates that each agent should be granted as few privileges as possible, under the constraint that all tasks can be done)** [Page 73].

Chan et al. is directed towards creating and developing workflows based on contracts that specify the relationship between workflows and workflow steps (i.e., workflow specification), whereas Patrick is directed towards considering access control security in providing the development of secure workflow. Thus, both Chan et al. and Patrick are deemed to be related towards different aspects of workflow development. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Chan et al. to include the steps of calculating the exposure measure of each workflow and selecting the workflow with the smallest

(minimum) exposure measure, as taught by Patrick, because doing so enhances the teachings of Chan et al. by integrating the concept of least privilege, granting only those privileges that are necessary to accomplish the task at hand, in order to provide the resultant high degree of security, facilitate hamper-free execution of workflows, and provide mechanisms to design systems that meet user's requirements for maintaining a high degree of security while getting workflows executed, as taught by Patrick [pages 66-67].

As per claim 2, Chan et al. teaches the method as claimed in claim 1, further comprising the step of storing a library of components from which possible workflows can be constructed **(The display may include a palette of workflow steps 109 that may be selected to build or edit a workflow 108 by, for example, a drag-and-drop operation. Design-time container 110 retrieves workflow steps 109 from workflow library 111 and inserts them into workflow 108 as a user designs workflow 108; Palette window 156 provides a list of the workflow steps 109 available for designing workflows 108. Workflow steps 109 may be placed in folders to organize the steps 109)** [Column 3, lines 21-27, Column 6, lines 14-22].

As per claim 3, although not explicitly taught by Chan et al., Patrick teaches the method as claimed in claim 1, further comprising the step of defining an exposure measure to be representative of an amount of information that a constructed workflow

exposes **(We define Security Risk Factor to be the maximum number of tasks done by any one agent)** [Page 73].

Chan et al. is directed towards creating and developing workflows based on contracts that specify the relationship between workflows and workflow steps (i.e., workflow specification), whereas Patrick is directed towards considering access control security in providing the development of secure workflow. Thus, both Chan et al. and Patrick are deemed to be related towards different aspects of workflow development. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Chan et al. to include the steps of calculating the exposure measure of each workflow and selecting the workflow with the smallest (minimum) exposure measure, as taught by Patrick, because doing so enhances the teachings of Chan et al. by integrating the concept of least privilege, granting only those privileges that are necessary to accomplish the task at hand, in order to provide the resultant high degree of security, facilitate hamper-free execution of workflows, and provide mechanisms to design systems that meet user's requirements for maintaining a high degree of security while getting workflows executed, as taught by Patrick [pages 66-67].

As per claim 4, Chan et al. does not explicitly teach the method as claimed in claim 1, further comprising the step of defining an exposure measure to be representative of a duration for which a constructed workflow exposes information.

Patrick discusses the concept of least privilege, where users are given access privileges only long enough to perform the task assigned to them **(ideally, the agent would be allowed to write d only when he is actively engaged in task t. In the workflow, the agent who is assigned to the task dynamically (i.e., at runtime) is granted the least privileges to the documents required for the execution of the task. Therefore, the agent can access those required documents during the execution of the task. These privileges are then revoked from the agent after it has finished performing the task)** [Pages 81-82], and provides quantifiable measures regarding the exposure of a workflow **(We define Security Risk Factor to be the maximum number of tasks done by any one agent)** [Page 73], but does not explicitly teach the step of defining an exposure measure as representative of a duration for which a constructed workflow exposes information.

However, Official Notice is taken that using quantifiable methods to measure data describing the state or performance of a system or process, such as length, duration, or amount of an event or output, is old and well known in the art. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Chan et al. to include the steps of defining an exposure measure of each workflow to be representative of a duration for which a workflow exposes information, because doing so enhances the teachings of the concept of least privilege, as taught by Patrick, by providing a quantifiable measure that allows a

quantifiable comparison of exposure duration for benchmarking and establishing maximum thresholds as a basis for redesigning workflow to become more secure and abide by the principle of least privilege taught by Patrick, and further enables organizations to focus their risk management efforts strategically by quantifying and demonstrating improvement and enhanced security of workflows, and tracking performance over time.

Further, one of ordinary skill in the art would have recognized that applying the known technique of applying quantitative measures to the teachings of Chan et al. and Patrick would have yielded predictable results because the level of ordinary skill in the art demonstrated by the references applied shows the ability to incorporate quantitative measures describing the exposure "measure". Further, applying a quantitative measure to measure the length or duration of time information is exposed would have been recognized by those of ordinary skill in the art as resulting in an improved system that would allow more quantifiable comparison of exposure duration for benchmarking and establishing of maximum thresholds as a basis for redesigning workflow to become more secure and abide by the principle of least privilege taught by Patrick, enabling organizations to focus their risk management efforts strategically by quantifying and demonstrating improvement and enhanced security of workflows, and tracking performance over time.

As per claim 5, although not explicitly taught by Chan et al., Patrick teaches the method as claimed in claim 1, further comprising the step of defining an exposure measure to be representative of an amount of information that a constructed workflow exposes **(We define Security Risk Factor to be the maximum number of tasks done by any one agent)** [Page 73].

Chan et al. is directed towards creating and developing workflows based on contracts that specify the relationship between workflows and workflow steps (i.e., workflow specification), whereas Patrick is directed towards considering access control security in providing the development of secure workflow. Thus, both Chan et al. and Patrick are deemed to be related towards different aspects of workflow development. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Chan et al. to include the steps of calculating the exposure measure of each workflow and selecting the workflow with the smallest (minimum) exposure measure, as taught by Patrick, because doing so enhances the teachings of Chan et al. by integrating the concept of least privilege, granting only those privileges that are necessary to accomplish the task at hand, in order to provide the resultant high degree of security, facilitate hamper-free execution of workflows, and provide mechanisms to design systems that meet user's requirements for maintaining a high degree of security while getting workflows executed, as taught by Patrick [pages 66-67].

Patrick discusses the concept of least privilege, where users are given access privileges only long enough to perform the task assigned to them **(ideally, the agent would be allowed to write d only when he is actively engaged in task t. In the workflow, the agent who is assigned to the task dynamically (i.e., at runtime) is granted the least privileges to the documents required for the execution of the task. Therefore, the agent can access those required documents during the execution of the task. These privileges are then revoked from the agent after it has finished performing the task)** [Pages 81-82], and provides quantifiable measures regarding the exposure of a workflow **(We define Security Risk Factor to be the maximum number of tasks done by any one agent)** [Page 73], but does not explicitly teach the step of defining an exposure measure as representative of a duration ***and*** amount for which information is exposed for a constructed workflow.

However, Official Notice is taken that using quantifiable methods to measure data describing the state or performance of a system or process, such as length, duration, or amount of an event or output, or a combination of multiple descriptive measures, is old and well known in the art. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Chan et al. to include the steps of defining an exposure measure of each workflow to be representative of a duration and amount of information exposed by a workflow, because doing so enhances the teachings of the concept of least privilege, as taught by Patrick, by providing a quantifiable measure that allows a quantifiable comparison of exposure

duration for benchmarking and establishing maximum thresholds as a basis for redesigning workflow to become more secure and abide by the principle of least privilege taught by Patrick, and further enables organizations to focus their risk management efforts strategically by quantifying and demonstrating improvement and enhanced security of workflows, and tracking performance over time.

Further, one of ordinary skill in the art would have recognized that applying the known technique of applying quantitative measures to the teachings of Chan et al. and Patrick would have yielded predictable results because the level of ordinary skill in the art demonstrated by the references applied shows the ability to incorporate quantitative measures describing the exposure "measure". Further, applying a quantitative measure to measure the length or duration of time information is exposed would have been recognized by those of ordinary skill in the art as resulting in an improved system that would allow more quantifiable comparison of exposure duration for benchmarking and establishing of maximum thresholds as a basis for redesigning workflow to become more secure and abide by the principle of least privilege taught by Patrick, enabling organizations to focus their risk management efforts strategically by quantifying and demonstrating improvement and enhanced security of workflows, and tracking performance over time.

Claim 6 recites limitations already addressed by the rejection of claim 1 above; therefore, the same rejection applies.

Further, the teachings of Chan et al. are embodied as a computer-based system, evidenced by its use within a communications network **(telecommunications device 120 communicates with system 104 through a communications network 122 such as a local, wide, or global area network, a private branch exchange, a public switched telephone network, wired and/or wireless communication links, and/or any combination of the previously mentioned communication links)** and use of Java based programming **(Microsoft Windows Foundation Class or Java Foundation Class may be used by design-time container 110)** and other computing-based structures **(run-time container, design time container)** [Column 2, lines 37-47, Column 3, lines 20-21, claim 1].

Claim 7 recites limitations already addressed by the rejection of claim 1 above; therefore, the same rejection applies.

Further, the teachings of Chan et al. are embodied within application development software embodied in a computer-readable medium [Claim 15].

Claim 8 recites limitations already addressed by the rejection of claim 2 above; therefore, the same rejection applies.

Claim 9 recites limitations already addressed by the rejection of claim 3 above; therefore, the same rejection applies.

Claim 10 recites limitations already addressed by the rejection of claim 4 above; therefore, the same rejection applies.

Claim 11 recites limitations already addressed by the rejection of claim 5 above; therefore, the same rejection applies.

Claim 12 recites limitations already addressed by the rejection of claim 2 above; therefore, the same rejection applies.

Claim 13 recites limitations already addressed by the rejection of claim 3 above; therefore, the same rejection applies.

Claim 14 recites limitations already addressed by the rejection of claim 4 above; therefore, the same rejection applies.

Claim 15 recites limitations already addressed by the rejection of claim 5 above; therefore, the same rejection applies.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Redlich et al. (US Patent #7,140,044) teaches a data security system and method for separation of user communities.

Ernst (US Patent #5,890,133) teaches a method and apparatus for dynamic optimization of business processes managed by a computer system that collects, investigates and stores parameters, data, and result data, and subsequently optimizes business processes on the basis of stored information by identifying a business process instance having propitious result data, modifying the parameters of said instance and subsequent verification of such modification.

Tracy et al. (UGPGPub 2003/0050718) teaches an enhanced system, method and medium for certifying and accrediting requirements compliance. System configuration information is gathered and assessed according to selected requirements and associated test procedures. At least one of a plurality of predefined process steps is selected to create a tailored sequence of process steps that can be used to assess the risk of and/or determine the suitability of a target system to comply with at least one predefined standard, regulation and/or requirement.

Patrick Hung and Kamalakar Karlapalem's "A Secure Workflow Model" (provided as reference 1-V) teaches that security requirements are particularly needed in workflow when the workflow manipulates confidential or sensitive information, the information moves in and out of a set of agents, and when there are authorization procedures for different resources that need to be enforced in the workflow.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PETER CHOI whose telephone number is (571)272-6971. The examiner can normally be reached on M-F 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Beth Van Doren can be reached on (571) 272-6737. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

June 5, 2008

/P. C./
Examiner, Art Unit 3623

/Romain Jeanty/
Primary Examiner, Art Unit 3623